

KSC

Инструкции по интеграциям с KSC

- [Интеграция KUMA с KSC](#)
- [KSC: увеличение лимита экспорта событий в SIEM \(Syslog/CEF\)](#)

Интеграция KUMA с KSC

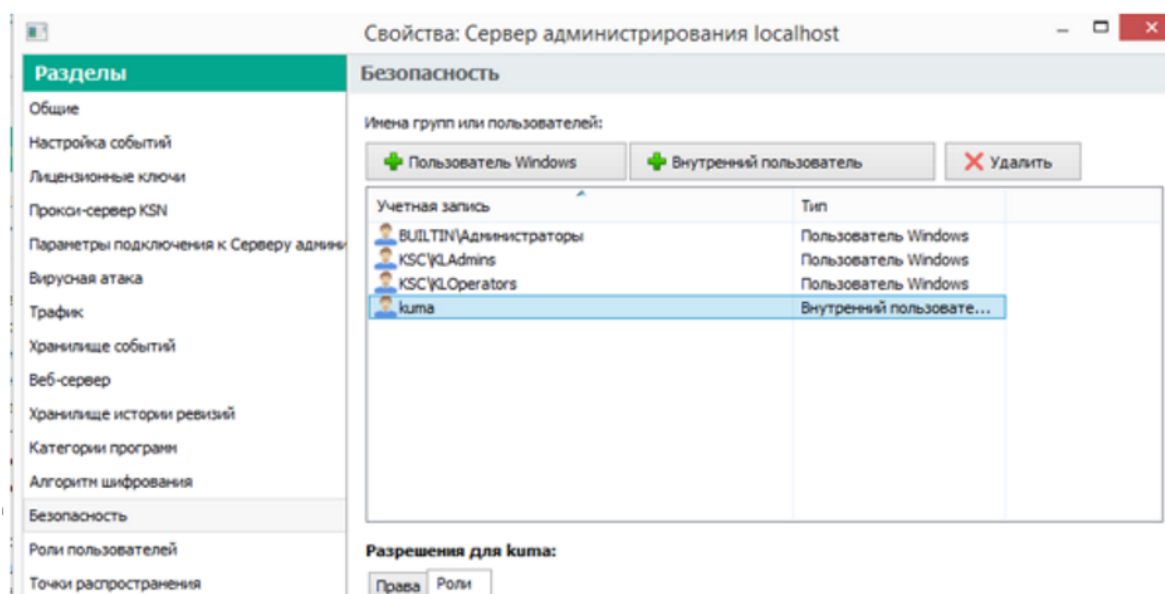
Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Официальная документация по данному разделу приведена в Онлайн-справке на продукт: <https://support.kaspersky.com/KUMA/2.1/ru-RU/217923.htm>

<https://www.youtube.com/embed/u6v3qbDmu2Q?si=8K7B8BzkDDmL7KnX>

Интеграция KUMA с KSC позволяет получить активы и данные по ним, которыми управляет KSC, возможность запуска задач реагирования, перемещение активов между группами KSC, закрытие уязвимостей (при наличии лицензии от Kaspersky Endpoint Security для бизнеса Расширенный и выше) из интерфейса KUMA.

Для интеграции необходимо заранее создать учетную запись (внутреннего пользователя) в KSC:



Допускается также использовать доменную учетную запись пользователя для интеграции KUMA с KSC. Учетная запись пользователя в секрете KUMA указывается в формате: username@domain

Если на KSC включено MFA, то нужно сделать исключение для учетки KUMA. Согласно этой инструкции: <https://support.kaspersky.com/help/KSC/14.2/ru-RU/211462.htm>

В дополнение к исключению MFA для интеграционной УЗ KUMA можно настроить список адресов, с которых разрешено подключение к KSC: <https://support.kaspersky.com/KSC/14.2/ru-RU/231374.htm>

Созданной учетной записи необходимо назначить определенный набор прав доступа к функциям Kaspersky Security Center. Это можно сделать одним из следующих способов:

- настроить права для учетной записи индивидуально;
- создать роль пользователя с настроенным набором прав и присвоить данную роль учетной записи, которая будет использоваться для интеграции.

Перечень минимальных прав представлен на рисунке ниже. Данный набор прав позволяет:

- выполнять импорт информации об активах;
- перемещать устройства между группами KSC;
- вручную запускать задачи поиска вредоносного ПО или обновления антивирусных баз из интерфейса KUMA;
- автоматически запускать задачи поиска вредоносного ПО или обновления антивирусных баз с помощью правил реагирования KUMA.

Имя	Разрешить	Запретить
Сервер администрирования Kaspersky Security Center	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Общий функционал	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Управление группами администрирования	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Запись	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Доступ к объектам независимо от их списков ACL	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Чтение	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Базовая функциональность	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Чтение	<input type="checkbox"/>	<input type="checkbox"/>
Запись	<input type="checkbox"/>	<input type="checkbox"/>
Выполнение	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Выполнение операций с выборками устройств	<input type="checkbox"/>	<input type="checkbox"/>
Удаленные объекты	<input type="checkbox"/>	<input type="checkbox"/>
Управление ключами шифрования	<input type="checkbox"/>	<input type="checkbox"/>
Обработка событий	<input type="checkbox"/>	<input type="checkbox"/>
Операции с Сервером администрирования	<input type="checkbox"/>	<input type="checkbox"/>
FUNC_AREA_HOST_TAGS	<input type="checkbox"/>	<input type="checkbox"/>
Развертывание программ "Лаборатории Касперского"	<input type="checkbox"/>	<input type="checkbox"/>
Управление лицензионными ключами	<input type="checkbox"/>	<input type="checkbox"/>
Интеграция программы	<input type="checkbox"/>	<input type="checkbox"/>
Управление отчетами	<input type="checkbox"/>	<input type="checkbox"/>
Иерархия Серверов администрирования	<input type="checkbox"/>	<input type="checkbox"/>
FUNC_AREA_SERVICE_ACCOUNTS	<input type="checkbox"/>	<input type="checkbox"/>
Права пользователей	<input type="checkbox"/>	<input type="checkbox"/>
Виртуальные Серверы администрирования	<input type="checkbox"/>	<input type="checkbox"/>
Mobile Device Management	<input type="checkbox"/>	<input type="checkbox"/>
Управление системой	<input type="checkbox"/>	<input type="checkbox"/>
Kaspersky Endpoint Security для Windows (12.1.0)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Адаптивный контроль аномалий	<input type="checkbox"/>	<input type="checkbox"/>
Компоненты защиты	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Чтение	<input type="checkbox"/>	<input type="checkbox"/>
Запись	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Выполнение	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Выполнение операций с выборками устройств	<input type="checkbox"/>	<input type="checkbox"/>
Контроль программ	<input type="checkbox"/>	<input type="checkbox"/>
Базовая функциональность	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Чтение	<input type="checkbox"/>	<input type="checkbox"/>
Запись	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Выполнение	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Выполнение операций с выборками устройств	<input type="checkbox"/>	<input type="checkbox"/>
Detection and Response	<input type="checkbox"/>	<input type="checkbox"/>
Контроль устройств	<input type="checkbox"/>	<input type="checkbox"/>
Шифрование	<input type="checkbox"/>	<input type="checkbox"/>
Предотвращение вторжений	<input type="checkbox"/>	<input type="checkbox"/>
Исключения	<input type="checkbox"/>	<input type="checkbox"/>
Веб-Контроль	<input type="checkbox"/>	<input type="checkbox"/>

Права пользователю нужно выдавать не только в свойствах KSC, но и в свойствах групп управляемых устройств, убедитесь, что не отключено наследование, чтобы права корректно распространялись на подгруппы

На стороне KUMA необходимо указать адрес и порт 13299 (этот порт используется по умолчанию), а также УЗ, о которой говорилось выше.

Параметры подключения

*Название
KSC

*URL
10.68.85.30:13299

*Секрет
KSC Integration

☐ Выключено

Иерархия

☒ Импортировать активы из новых групп

+ 10.68.85.30

При нажатии в KUMA на кнопку "Сохранить", не должно всплывать сообщений об ошибке.

KSC: увеличение лимита экспорта событий в SIEM (Syslog/CEF)

Официальная документация по настройке автоматического экспорта событий в SIEM-системы: <https://support.kaspersky.ru/ksc/14.2/151333>

?? ?????????? KSC ?????? ??????? ?? Syslog ?? ????? 100 ???? ??????? 30 ??????. ??? ??????? ?????????? ?????????? ?????????? ?/??? ?????????????? ??????? ?????? ??????????? ??????????, ?????? ????????? ? KSC ?????? ?? ?????????? ?????????????? ? SIEM, ? ?????? ?????????? ?????????? ?????????? ?? ??????????.

Изменить значение по экспорту событий, можно в реестре в системе с установленным Сервером администрирования.

Раздел:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

Флаги:

- KLSPLG_READ_MAX_COUNT_SF - количество событий, обрабатываемых в каждой итерации. Значение по умолчанию - 100 (в десятичной форме)
- KLSPLG_READ_DB_PERIOD_SF - скорость итерации в миллисекундах. По умолчанию 30000 (в десятичной форме).

?????????? ? ?????????? ?????????? ?? ?????????? ?????? ? ??????????????????. ?????????? ?????????? ?????? ?????????? ?? ?????? ?????????????????????????? ??????????. ?????????????????? ?????????????? ?????????????? ??????????, ?????????????? ?????? ??? ?? KSC, ??? ? ?? ??? ????